WHITELIST ACCESS REQUEST
Guidelines

TABLE OF CONTENTS

1 PURPOSE

The Office of Information Technology (OIT) supports two anti-spam devices from IronMail that filter and quarantine nuisance spam email coming from the Internet into State network. A "WhiteList" is a list of email sources that are exempt from Anti-SPAM filtering. The purpose of this guideline is to establish and maintain consistent procedures to facilitate requests for adding email addresses to the WhiteList. The implementation of CipherTrust's IronMail Anti-SPAM appliances will detect and identify some web newsletters and group e-mails as SPAM. Marked as SPAM, these e-mails quarantined as SPAM. The following day, the State employee will receive an e-mail report (possibly two reports – one report from each appliance) for all SPAM received during the prior 24-hour period. At this point, the State employee has the option to release any e-mail identified in the report(s). This release causes the e-mail to be released to all State employees listed in the e-mail as a receiver. This request allows the sender of the e-mail to be included on the WhiteList in the IronMail appliances which by-passes all SPAM filtering and allows for immediate delivery.

2 REQUESTING WHITELIST ACCESS

To request an e-mail sender address to be added to the WhiteList, complete the following steps:

1. The authorized user shall call Help Desk Services (HDS) at 271-7555 to log an official request and obtain a ticket number. All WhiteList access requests must have a ticket number for verification purposes. Any requests that do not have a ticket number will not be processed.
2. Ticket requests will be routed to Groupware Support Services (GSS) and placed on HOLD until appropriate approvals and authorizations have been received. ***If the appropriate documentation is not received within 20 days of the creation date, you will receive notification from the GSS Unit that your request will be closed within 48 hours.***
3. Requesting user shall complete the WhiteList Access Request form, which is available as a Word document on this Website, and **submit it via email**.

3 APPROVAL

To obtain required approval for your WhiteList access request complete the following steps:

NOTE: ANY REQUESTS THAT DO NOT FOLLOW THE POLICY GUIDELINES WILL BE SUBJECT TO DELAYS AND/OR NOT BE PROCESSED.

1. User shall complete and submit, the WhiteList Access Request form to their immediate supervisor **via email** for approval, with a carbon copy to IronMail@oit.nh.gov.
2. If approved, the user's immediate supervisor shall forward the completed WhiteList Access Request form **via email** to their Authorizing Agency/Director for approval.
3. If approved, the Authorizing Agency/Director shall forward the completed WhiteList Access Request form **via email** to the Chief Information Officer, Richard C. Bailey, Jr., and a carbon copy to his assistant, Patricia Bernard.

Note: Do not forward requests to GSS. All requests must be reviewed and approved by the Division Director and Chief Information Officer. Any requests that do not have the appropriate approvals will not be processed.

4 AUTHORIZATION

1. Chief Information Officer receives authorization email message from the Division Director, with the electronic copy of the request form attached.
2. Chief Information Officer reviews the request.
    a. If the request is denied, the request will be returned to the Division Director with a carbon to GSS (IronMail@oit.nh.gov).
    b. If the request is approved, the Chief Information Officer shall forward the authorized request to GSS for a WhiteList creation for the provided e-mail Sender.

5 WHITELIST CREATION

1. The GSS Unit receives the authorized request notification and the electronic version of the request form from the Chief Information Officer.
2. GSS Unit shall verify that an official ticket has been logged based on the ticket number provided on the WhiteList access request form.
3. Ticket shall be routed to a technician for WhiteList access creation.
4. Upon completion, technician shall update ticket details and close ticket. Technician shall update the request form, enter completion date and retain form in the records keeping folder. WhiteList spreadsheet for domain\senders will be updated for each division and the State.

6 WHITELIST ACCESS CONFIRMATION

1. Technician shall forward notification to user, via e-mail, confirming WhiteList entry creation.
2. User confirmation based on frequency of delivery that e-mail by-passed all SPAM checking.

7 WHITELIST ACCESS REQUEST FORM

1. To submit your request, use the WhiteList Request Form available on this Website.